

Words on finite nilpotent groups of class 2

Ainhoa Iñiguez Goizueta

Abstract

Let G be a finite nilpotent group of class at most 2, and let $w = w(x_1, \dots, x_n)$ be a group word in n variables. Then we prove that the number of solutions in $G \times \dots \times G$ to the equation $w = 1$ is at least $|G|^{n-1}$. This result, also independently obtained by Matthew Levy [L], solves a special case of a conjecture of Alon Amit.

1 Introduction

If $w = w(x_1, \dots, x_n)$ is a group word, then for every group G we have a verbal mapping

$$\begin{aligned} w &: G^{(n)} &\longrightarrow & G \\ (g_1, \dots, g_n) &\longmapsto & w(g_1, \dots, g_n) \end{aligned}$$

by substitutions of the n -tuples.

We use the notation $N(G, w)$ for the number of solutions to the equation $w = 1$ in the group G , that is, for the cardinality of $w^{-1}(1)$. More generally, if S is a subset of $G^{(n)}$, we write $N(S, w)$ for the number of solutions to $w = 1$ lying in S . Thus $N(G, w)$ can be seen as a shortcut for $N(G^{(n)}, w)$.

If G is abelian, then the verbal mapping $w : G^{(n)} \rightarrow G$ is a homomorphism and so each non-empty fibre $w^{-1}(g)$ is a coset of the kernel $w^{-1}(1)$. Besides, since G is also finite (a) $|w^{-1}(1)| \geq |G^{(n)}|/|G|$ and (b) all non-empty fibres have the same size. If G is finite and nilpotent, but not abelian, then (b) is no longer true in general. Whether (a) still holds is an open problem (that it does is conjectured by Amit [A]). The aim of this paper is to show that the conjecture of Amit is true for finite groups of nilpotency class at most 2.

Theorem 1. *Let G be a finite group of nilpotency class at most 2, and let $w = w(x_1, \dots, x_n)$ be a group word. Then $N(G, w) \geq |G|^{n-1}$.*

If the theorem holds for two groups A and B of nilpotency class at most 2, then it holds for their direct product $G = A \times B$ since the word values can be solved componentwise.

Let $\mathbf{g} = \mathbf{a} \cdot \mathbf{b} = (a_1, \dots, a_n) \cdot (b_1, \dots, b_n) \in A^{(n)} \times B^{(n)} = G^{(n)}$, then $w(\mathbf{g}) = w(\mathbf{a}) \cdot w(\mathbf{b})$ which implies $N(G, w) \geq N(A, w) \cdot N(B, w)$ and the result follows

from $|G| = |A| \cdot |B|$. Any finite nilpotent group is a direct product of its Sylow subgroups. Hence it will be enough to show the theorem for p -groups:

Theorem 2. *Let G be a finite p -group of nilpotency class at most 2, and let $w = w(x_1, \dots, x_n)$ be a group word. Then $N(G, w) \geq |G|^{n-1}$.*

This result was also independently obtained by Matthew Levy [L].

2 Useful lemmas

If w_1, \dots, w_k is a finite family of words in the same variables x_1, \dots, x_n , then we can consider the mapping

$$\begin{aligned} f_{w_1, \dots, w_k} : G^{(n)} &\longrightarrow G^{(k)} \\ (g_1, \dots, g_n) &\longmapsto (w_1(g_1, \dots, g_n), \dots, w_k(g_1, \dots, g_n)). \end{aligned}$$

On the other hand, if $w = w(x_1, \dots, x_n)$ and u_1, \dots, u_n are words in the same variables y_1, \dots, y_k , then we can define the *composition* $w(u_1, \dots, u_n)$, which results from substituting each word u_i for the indeterminate x_i in the expression for w . In other words, if F is the free group on x_1, \dots, x_n and F^* is the free group on y_1, \dots, y_k , then $w(u_1, \dots, u_n)$ is the image of w under the homomorphism $F \rightarrow F^*$ sending each x_i to u_i .

Lemma 3. *Let $w = w(x_1, \dots, x_n)$ and u_1, \dots, u_n be group words, and put $w' = w(u_1, \dots, u_n)$. If G is a group for which the map f_{u_1, \dots, u_n} is bijective, then we have $N(S, w') = N(S, w)$ for every subset S of $G^{(n)}$.*

Proof. This is clear, since $f_{w'}$ is the composition of f_{u_1, \dots, u_n} and f_w . \square

The previous lemma will be used in conjunction with the following one. Recall that, if G is a finite p -group and m is an integer which is not divisible by p , then the map $g \mapsto g^m$ is bijective. This is an immediate consequence of Bézout's identity.

Lemma 4. *Let u_1, \dots, u_n be words of the form $u_i = x_i^{m_i} v_i$, where v_i is a word which only depends on x_{i+1}, \dots, x_n . If G is a finite p -group and $(m_i, p) = 1$ for every $i = 1, \dots, n$, then the mapping f_{u_1, \dots, u_n} is bijective on $G^{(n)}$.*

Proof. Since f_{u_1, \dots, u_n} goes from $G^{(n)}$ to $G^{(n)}$, it suffices to prove that it is an injective map. If (g_1, \dots, g_n) and (h_1, \dots, h_n) are two tuples with the same image under f_{u_1, \dots, u_n} , we prove that $g_i = h_i$ for all $i = 1, \dots, n$ by reverse induction on i . For $i = n$ this is an immediate consequence of the remark preceding this lemma, since the word u_n is of the form $x_n^{m_n}$ with $(m_n, p) = 1$. Assume now that $g_{i+1} = h_{i+1}, \dots, g_n = h_n$, and let us see that $g_i = h_i$. Since $u_i(g_i, \dots, g_n) = u_i(h_i, \dots, h_n)$ and $u_i = x_i^{m_i} v_i$ for a word v_i involving only x_{i+1}, \dots, x_n , it follows that $g_i^{m_i} = h_i^{m_i}$, and we conclude that $g_i = h_i$ as before. \square

Of course, the previous lemma admits variations which follow by reordering the variables. For example, if $n = 3$ and $u_1 = x_1$, $u_2 = x_2x_1$, $u_3 = x_3x_2$, then the map f_{u_1, u_2, u_3} is bijective on $G^{(3)}$.

The following result will also be used on several occasions. The proof is obvious.

Lemma 5. *Let w be a group word in the free group F , and let G be a finite p -group of order p^n and class c . If w' is a word such that $w \equiv w' \pmod{\gamma_{c+1}(F)F^{p^n}}$, then $f_w = f_{w'}$ on $G^{(n)}$.*

As a consequence, if G is a finite p -group of class 2 and we want to study the number $N(G, w)$ for a group word w , we may assume without loss of generality that w is of the form

$$x_1^{k_1} \dots x_n^{k_n} \prod_{1 \leq i < j \leq n} [x_i, x_j]^{k_{ij}}.$$

Also, if $w = u^k v$ for some words u and v and for some exponent k , then we may replace k with any other integer k' such that $k \equiv k' \pmod{|G|}$.

In the next theorem we consider a particular kind of words, which will be crucial for the proof of our main result. We need the following very simple lemma.

Lemma 6. *Let G be a nilpotent group of class at most 2, and let g be an element of G . Then $[g, G] = \{[g, h] \mid h \in G\}$, and every element of $[g, G]$ can be represented in $|C_G(g)|$ different ways in the form $[g, h]$ with $h \in G$. Hence $|[g, G]| = |G : C_G(g)|$.*

Proof. The equality $[g, G] = \{[g, h] \mid h \in G\}$ follows from the fact that the commutator is multilinear in a nilpotent group of class at most 2. On the other hand, since

$$[g, h_1] = [g, h_2] \iff g^{h_1} = g^{h_2} \iff h_1 h_2^{-1} \in C_G(g) \iff C_G(g)h_1 = C_G(g)h_2,$$

the elements which give the same commutator with g form a right coset of $C_G(g)$. Thus the number of different representations of a commutator with g coincides with the order of $C_G(g)$. \square

3 Proof of the theorem

Let's first show the proof for a particular word which is the main step in the main proof:

Theorem 7. *Let G be a finite p -group of class at most 2, and let w be a group word of the form*

$$w = x_1^m \prod_{2 \leq i < j \leq n} [x_i, x_j]^{k_{ij}}. \quad (1)$$

Then $N(G' \times G^{(n-1)}, w) \geq |G|^{n-1}$.

Proof. We argue by induction on n , the case $n = 1$ being trivial. Due to the form of the word w , it is impossible to have $n = 2$, so we suppose now that $n \geq 3$. In particular, we may assume that not all the exponents k_{ij} are 0. Choose the pair (r, s) such that the p -part of the exponent k_{rs} is as small as possible. By renaming the variables, we may assume that $r = n - 1$ and $s = n$. For simplicity, let us write k for $k_{n-1, n}$. For every pair (i, j) with $2 \leq i < j \leq n$, let k'_{ij} be a solution to the congruence

$$k'_{ij}k \equiv k_{ij} \pmod{|G|}.$$

(Such a solution exists by the choice of (r, s) , and because $|G|$ is a power of p .) By the remark preceding Lemma 5, we may assume that

$$w = x_1^m \prod_{2 \leq i < j \leq n} [x_i, x_j]^{k'_{ij}k}.$$

In the previous expression, we collect all commutators which contain either x_{n-1} or x_n , and get

$$w = x_1^m v [x_{n-1}, x_n]^k [x_{n-1}, v_{n-1}]^k [v_n, x_n]^k,$$

for some words v , v_{n-1} , and v_n involving only the variables x_i with $2 \leq i \leq n-2$. Thus

$$w = x_1^m v' [x_{n-1} v_n, x_n v_{n-1}]^k,$$

where $v' = [v_{n-1}, v_n]^k v$ again only involves x_2, \dots, x_{n-2} . Now, by using Lemmas 3 and 4 with $u_{n-1} = x_{n-1} v_n$, $u_n = x_n v_{n-1}$ and $u_i = x_i$ for $i = 1, \dots, n-2$ (see the remark after Lemma 4), we get $N(G' \times G^{(n-1)}, w) = N(G' \times G^{(n-1)}, w')$ for the word

$$w' = x_1^m v' [x_{n-1}, x_n]^k = x_1^m v' [x_{n-1}^k, x_n].$$

Since $w'' = x_1^m v'$ is of the form in the statement of the theorem and involves $n-2$ variables, the result is true for w'' . On the other hand,

$$\begin{aligned} N(G' \times G^{(n-1)}, w) &= \left| \{(g_1, \dots, g_n) \in G' \times G^{(n-1)} \mid w''(g_1, \dots, g_{n-2}) = [g_{n-1}^k, g_n]^{-1}\} \right|. \end{aligned}$$

By Lemma 6, each element of the commutator subgroup $[g_{n-1}^k, G]$ is of the form $[g_{n-1}^k, g_n]$, and there are $|C_G(g_{n-1}^k)|$ choices of g_n giving rise to the same element. Consequently,

$$\begin{aligned} N(G' \times G^{(n-1)}, w) &= \sum_{g_{n-1} \in G} |C_G(g_{n-1}^k)| \left| \{(g_1, \dots, g_{n-2}) \in G' \times G^{(n-3)} \mid w''(g_1, \dots, g_{n-2}) \in [g_{n-1}^k, G]\} \right|. \end{aligned}$$

Now, if we put $\overline{G} = G/[g_{n-1}^k, G]$, we have

$$\begin{aligned} &\left| \{(g_1, \dots, g_{n-2}) \in G' \times G^{(n-3)} \mid w''(g_1, \dots, g_{n-2}) \in [g_{n-1}^k, G]\} \right| \\ &= |[g_{n-1}^k, G]|^{n-2} N(\overline{G}' \times \overline{G}^{(n-3)}, w''). \end{aligned}$$

Since the result is true for w'' , we get

$$\begin{aligned}
N(G' \times G^{(n-1)}, w) &\geq \sum_{g_{n-1} \in G} |C_G(g_{n-1}^k)| |[g_{n-1}^k, G]|^{n-2} |\overline{G}|^{n-3} \\
&= \sum_{g_{n-1} \in G} |C_G(g_{n-1}^k)| |[g_{n-1}^k, G]| |G|^{n-3} \\
&= \sum_{g_{n-1} \in G} |G|^{n-2} = |G|^{n-1},
\end{aligned}$$

where we have used again Lemma 6. \square

Theorem 8. *Let G be a finite p -group of class at most 2, and let $w = w(x_1, \dots, x_n)$ be a group word. Then $N(G, w) \geq |G|^{n-1}$.*

Proof. By working in the abelian group F/F' , we can write $w = (x_1^{k_1} \dots x_n^{k_n})^m v$, where $v \in F'$, m is a power of p , and at least one k_i is not divisible by p . After renaming the variables if necessary, we may assume that $i = 1$. If we put

$$u_1 = x_1^{k_1} \dots x_n^{k_n}, \quad u_2 = x_2, \quad \dots, \quad u_n = x_n,$$

then we can apply Lemmas 3 and 4 to obtain $N(G, w) = N(G, w')$, where now w' is of the form $w' = x_1^m v'$, for some word $v' \in F'$. Since G has class at most 2, we may assume that v' is of the form

$$\prod_{1 \leq i < j \leq n} [x_i, x_j]^{k_{ij}}.$$

We can write $v' = [x_1, v'_1]v'_2$, where v'_1 and v'_2 depend only on x_2, \dots, x_n , and where $v'_2 \in F'$. If we put $w'' = x_1^m v'_2$, then $N(G, w) \geq N(G' \times G^{(n-1)}, w'')$. Now the result follows by applying Theorem 7. \square

References

- [A] A. Amit, On equations in nilpotent groups, unpublished
- [L] M. Levy, On the probability of satisfying a word in nilpotent groups of class 2, <http://arxiv.org/abs/1101.4286>